ABSTRACT

Performance of a pattern-matching intrusion detection system (IDS) is improved by ranking signatures in its signature table by likelihood of occurrence, so that the table may be searched efficiently. Occurrence data associated with signatures is kept, and the ranking adaptively revised according to updates of the data. When the IDS detects a system event, the signature table is searched. If the search does not find a signature matching the event, thereby suggesting that the event poses no threat, a null signature is added to the signature table in a strategic location to terminate future searches early. In one embodiment, null signatures may be stored in a cache. When a system event is detected, the cache is searched. If a match is not found, the signature table is searched. If a match is not found in the signature table, a null signature is cached.